The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/12/2010

SUBJECT:
Multiple Vulnerabilities in Microsoft Windows OpenType Fonts (MS10-076 and MS10-078)

OVERVIEW:
Multiple vulnerabilities have been discovered in the Microsoft Windows OpenType Fonts that could allow for remote code execution. OpenType Fonts are fonts that get embedded in documents such as Microsoft Word, Power Point, or Web pages. These vulnerabilities can be exploited if a user visits a specially crafted webpage or opens a specially crafted file, including e-mail attachments.

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts.

SYSTEMS AFFECTED:
Windows XP
Windows Server 2003
Windows Vista
Windows Server 2008
Windows 7
Windows Server 2008 R2

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been identified in Microsoft Windows OpenType Fonts. The first vulnerability exists in the way the Microsoft Windows Embedded OpenType (EOT) Font Engine decompresses specially crafted EOT fonts that could allow for remote code execution. The second and third vulnerabilities exist due to the way that the Windows OpenType Font (OTF) format driver parses specially crafted OpenType fonts. These vulnerabilities could allow for an elevation of privileges, however, under certain circumstances these vulnerabilities may lead to remote code execution. These vulnerabilities can be exploited by visiting a specially crafted webpage or by opening a specially crafted file, such as an email attachment. In an email scenario the attacker would need the user to open an attachment or click a link to a specially crafted webpage.

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the appropriate patches provided by Microsoft immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/Bulletin/MS10-076.mspx
http://www.microsoft.com/technet/security/Bulletin/MS10-078.mspx

Security Focus:

http://www.securityfocus.com/bid/43775
http://www.securityfocus.com/bid/43778
http://www.securityfocus.com/bid/43779

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1883
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2740
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2741